Nonlinear, Nonbinary Cyclic Group Codes

G. Solomon[1]

New cyclic group codes of length $2^m - 1$ over (m − j)-bit symbols are introduced. These codes can be systematically encoded and decoded algebraically. The code rates are very close to Reed-Solomon (RS) codes and are much better than Bose-Chaudhuri-Hocquenghem (BCH) codes (a former alternative). The binary (m − j)-tuples are identified with a subgroup of the binary m-tuples which represent the field GF(2^m). Encoding is systematic and involves a two-stage procedure consisting of the usual linear feedback register (using the division or check polynomial) and a small table lookup. For low rates, a second shift-register encoding operation may be invoked. Decoding uses the RS error-correcting procedures for the m-tuple alphabet, i.e., the elements of the field GF(2^m). Appendices A and B list (m − j)-tuple codes for m = 4, 5, and 6.

I. Cyclic Group Codes of Length (2^m−1) Over Binary (m−1)-tuples

Group codes of lengths up to 2^m over binary $(m-1)$-tuples are introduced and are shown to be cyclic and systematically encodable. These $(m-1)$-tuples are identified with an additive subgroup of the field GF(2^m). These codes are not linear; that is, a codeword does not admit multiplication by a GF(2^m) field element to yield another codeword.

Consider the field GF(2^m) along with a primitive element β, which generates the $n = (2^m - 1)$ roots of unity. In addition, β is chosen with the following properties:

(1) m odd: Tr $\beta^i = 0$ for $1 \leq i \leq m-1$, where Tr denotes the linear field operator "trace." Tr $\beta = \beta + \beta^2 + \beta^4 + \cdots + \beta^{2m-1}$; thus, Tr $\beta \in$ GF(2), Tr β^2 = Tr β, and Tr cx^2 = Tr $\sqrt{c}x$, for $c, x \in$ GF(2^m).

(2) m even: Tr $\beta^i = 0$ for $0 \leq i \leq m-1$ except for a single odd integer p, $p < m$, and Tr $\beta^p = 1$.

The following are polynomials for β that satisfy the conditions (1) and (2) above for $3 \leq m \leq 12$.

m	Polynomial for β	Explanation
3	3 1 0	$(x^3 + x + 1)$
4	4 1 0	
5	5 3 0	
6	6 1 0	(Tr $\beta^5 = 1$)
7	7 3 0	
8	8 4 3 2 0	(Tr $\beta^5 = 1$)
9	9 5 0	
10	10 3 0	(Tr $\beta^7 = 1$)
11	11 9 0	
12	12 6 4 1 0	(Tr $\beta^{11} = 1$)

[1] Independent consultant to the Communications Systems Research Section.

Codes of length greater than 4096 are rarely invoked in present-day block-coding techniques. Do these properties extend beyond $m = 12$?

An element $c \in \mathrm{GF}(2^m)$ may be represented by $c = \sum_{i=0}^{m-1} c_i \beta^i$. One may identify Tr c by its binary representation (c_i); $0 \le i \le m-1$, and single out c_0 for m odd and c_p for m even. Thus, the binary value Tr c is determined by only the trace-one position (0 or p) in its binary m-bit representation.

Choose an $(n,\ k;\ d)$ Reed-Solomon (RS) code over $\mathrm{GF}(2^m)$ so that the codewords are values of sets of polynomials $P(x)$ with coefficients in $\mathrm{GF}(2^m)$ of fixed highest degree $(n-d)$ or $(n-d-1)$. A codeword $\mathbf{a} = (a_j)$ is represented by the values of a polynomial $P_{\mathbf{a}}(x)$ so that $a_j = P_{\mathbf{a}}(\beta^j)$, $0 \le j \le n-1$.

Restrict $P_{\mathbf{a}}(x)$ for all codewords $\mathbf{a}$ to an $(m-1)$ order subgroup of $\mathrm{GF}(2^m)$ by stipulating that Tr $P(x) = 0$ for $x \in \mathrm{GF}(2^m)$. Note that $P(x)$ as written here is generic for all $P_{\mathbf{a}}(x)$. The codes thus generated are cyclic group codes over $(m-1)$-bit symbols and are systematically encodable for codes meeting the conditions in the main theorem.

Example 1. Take the RS code $\mathbf{A}$ of dimension 5 over $\mathrm{GF}(2^m)$, $\mathbf{a} \in \mathbf{A}$, $\mathbf{a} = (a_i)$, and $a_i = P_{\mathbf{a}}(\beta^i)$. The polynomials $P_a(x)$ are of degree 4 with Tr $P_a(x) = 0$, for all $x \in \mathrm{GF}(2^m)$. For a general $P(x)$ and dropping the subscript $\mathbf{a}$, $P(x) = A + Bx + Cx^2 + Dx^3 + Ex^4$; $A, B, C, D, E \in \mathrm{GF}(2^m)$. The condition Tr $P_{\mathbf{a}}(x) = 0$ gives Tr $A = 0$, $B^4 + C^2 + E = 0$, and $D = 0$. This code has the binary dimension $(m-1) + 2m$.

For $m = 3$, one gets binary dimension 8 or dimension 4 over 2-tuples; i.e., a (7, 4; 3) code over binary doubles. This is a reduction from the (7, 5; 3) RS code over binary triples!

There exists no integer dimension over $(m-1)$-tuples for $m > 3$ since $(m-1) + 2m$ is not a multiple of $(m-1)$.

Example 2. Take an RS code of dimension 11 over GF(16) but choose as the Mattson-Solomon (M-S) set the polynomials $P(x)$ of degree 11, and set the constant term equal to zero. $P(x) = \sum_{i=1}^{11} c_i x^i$; Tr $P(x) = 0$ leads to

$$c_1^8 + c_2^4 + c_4^2 + c_8 = 0$$

$$c_3^4 + c_6^2 + c_9 = 0$$

$$c_5 + c_5^4 + c_{10}^2 + c_{10}^8 = 0$$

$$c_{11}^2 + c_7 = 0$$

The number of binary dimensions is 12 + 8 + 6 + 4 = 30, which is dimension 10 over binary triples. Thus, the (15, 11; 5) RS code over GF(16) is transformed into the nonsystematic (15, 10; 5) code over trace-zero elements of GF(16).

Example 3. Similarly, the RS (15, 7; 9) code over GF(16) using polynomials of degree 6 from 0 to 6, using analogous techniques, gives the relations

$$\text{Tr } c_0 = 0$$

$$c_1^4 + c_2^2 + c_4 = 0$$

$$c_6 + c_3^2 = 0$$

$$c_5 = 0$$

The binary dimension count is 3 + 8 + 4 = 15, which yields a (15, 5; 9) code over triples. Compare this with

(15, 5; 11) RS over 4-tuples,

(15, 5; 7) Bose-Chaudhuri-Hocquenghem (BCH) over GF(8) and GF(2), and

(15, 4; 10) BCH over GF(4) (doubles).

These nonsystematic codes are cyclic. Examine the conditions of the coefficients as in Example 2; for example, when a codeword $P(x)$ is shifted r positions to the left, the new polynomial $P'(x)$ that describes this new cycled codeword becomes $P'(x) = P(\beta^r x)$. If $P(x) = \sum c_i x^i$, then $d_i = c_i \beta^{ir}$ and

$$d_1^8 + d_2^4 + d_4^2 + d_8 = 0$$

$$d_3^4 + d_6^2 + d_9 = 0$$

$$d_5 + d_5^4 + d_{10}^2 + d_{10}^8 = 0$$

$$d_{11}^2 + d_7 = 0$$

$$d_1^8 + d_2^4 + d_4^2 + d_8 = \beta^{8r}(c_1^8 + c_2^4 + c_4^2 + c_8)$$

A. General Construction of These Cyclic Codes

To construct integer dimension codes of lengths up to 2^m over $(m-1)$-tuples with distance d, start with an RS code characterized by polynomials with M coefficients in $\mathrm{GF}(2^m)$. These polynomials are to be of degree $n-d$ or degree $n-d+1$ (if the constant term = 0). The RS $(n, k; d)$ code has $M = k$, $n = 2^m - 1$, and $k = n - d + 1$.

B. Conjugate Classes

Consider the map $x \rightarrow x^2$ and define the sets M_i for the odd integers i. Make them distinct:

$$M_i = \{\ i2^j \pmod{2^m - 1} : j = 0, 1, 2, \cdots, m-1\}$$

Each distinct set contains either m integers or some m_i integers where $m_i \mid m$. The M_i's are ordered in increasing i. For $m = 4$, the sets are $M_1 = \{1, 2, 4, 8\}$; $M_3 = \{3, 6, 9, 12\}$; $M_5 = \{5, 10\}$; and $M_7 = \{7, 11, 13, 14\}$.

The condition Tr $P(x) = 0$ translates into a condition on the integers in M_i that occurs as powers of x in the M-S polynomial. For each distinct set M_i there is a linear dependency. If all M_i have the same number of elements m, the effective k-dimension narrows down to $\deg P - r$ where r is the number of independent M_i's that occur in the powers of x. To yield an integer dimension, $m(\deg P - r)$ must be a multiple of $(m-1)$. Moreover, if $\deg P = n - d - 1$, one gets an additional dimension in this case since the condition Tr (constant) $= 0$ gives another set of $(m-1)$-tuples.

Example 4. In this example, $m = 5$ and codes are over 4-tuples. Start with (31, 27; 5) RS code over GF(32). The M-S polynomials here are of degree 26 and include the constant term. $M_1 = \{1\ 2\ 4\ 8\ 16\}$; $M_3 = \{3\ 6\ 12\ 24\ 17\}$; $M_5 = \{5\ 10\ 20\ 9\ 18\}$; $M_7 = \{7\ 14\ (28)\ 25\ 19\}$; $M_{11} = \{11\ 22\ 13\ 26\ 21\}$; and $M_{15} = \{15\ (30\ 29\ 27)\ 23\}$. Integers in parentheses indicate powers omitted in the M-S polynomials.

With degree of $P(x) = 26$, code dimension $k = 27$, and $r = 6$. Here one has a (31, 26; 5) code. This is obtained as follows: $26 - 6 = 20$ (5-tuples) and $20 \times 5 = 25 \times 4 = 25$ (4-tuples). Add the constant term to obtain 26 4-tuples. Since $\deg P(x) = 26$, the 4-tuple code obtained is the (31, 26; 5) code. This code is cyclic and nonsystematic when encoded via the coefficients of the polynomials $P(x)$. There are ways to encode systematically.

Example 5. Using similar arguments, one obtains

$\deg P(x)$	m	r	Code over 4-tuples
22	23	6	(31, 21; 9)
18	19	6	(31, 16; 13)
13	13	5	(31, 10; 19)

The full list of length-31 codes appears in Appendix A.

C. Alternate Construction

Consider generator polynomial $g(x)$ with roots as powers of powers of β in either the set $\mathbf{A} = \{1, 2, 3, 4, \ldots, 2t\}$ or $\mathbf{B} = \{0, 1, 2, 3, \ldots, 2t-1\}$. Choose $\mathbf{A}$ for m odd and $\mathbf{B}$ for m even. Examine the conjugate classes M_i that intersect $\mathbf{A}$ or $\mathbf{B}$. Let N_i be the number of elements in these M_i, and let A_i stand for the number in $M_i \cap \mathbf{A}$ or $M_i \cap \mathbf{B}$. There are $(N_i - A_i - 1)$ remaining independent constants for each i to be summed over the relevant i. Call this sum T: $T = \sum(N_i - A_i - 1)$. If $Tm = S(m-1)$ for S an integer, then the dimension of the entire $(m-1)$-tuple t-error correcting code is $S +$ dim of t-error correcting BCH code over m-tuples. $\mathbf{A}$ or $\mathbf{B}$ is chosen so that $Tm/(m-1)$ is an integer.

Example 6. Let $m = 4$ and β be a root of $x^4 + x + 1 = 0$. Let the generator polynomial contain $\mathbf{A} = \{\beta^i : 0 \leq i \leq 3\}$. $M_1 = \{1\ 2\ 4\ 8\}$; $M_3 = \{3\ 6\ 9\ 12\}$; $M_1 \cap \mathbf{A} = \{1, 2\}$; and $M_3 \cap \mathbf{A} = \{3\}$. $T = (4 - 2 - 1) + (4 - 1 - 1) = 3$ and $S = 3 \times 4/3 = 4$. One therefore has a contribution of four dimensions over 3-tuples. Add this to the BCH code of dimension 6, which does the regular job, and obtain a (15, 10; 5) cyclic code over triples.

Example 7. Let $m = 7$; $\mathbf{A} = \{1, 2, 3, 4, 5, 6\}$; β is a root of $x^7 + x^3 + 1$. Start by asking for a 3-error correcting code.

$$M_1 \cap A = \{1, 2, 4\};\quad M_1 = \{1, 2, 4, 8, 16, 32, 64\}$$

$$M_3 \cap A = \{3, 6\};\quad M_3 = \{3, 6, 12, 24, 48, 96, 65\}$$

$$M_5 \cap A = \{5\};\quad M_5 = \{5, 10, 20, 40, 80, 160, 33, 66\}$$

Therefore, one can have (3 of 7) + (4 of 7) + (5 of 7) linearly independent binary dimensions $= 12 \times 7 = 14 \times 6$. Now consider the (127, 106; 7) BCH code over 6-tuples, which contain none of the elements of M_i; $i = 1, 2, 3$. Thus, one has a total of 120 dimensions over 6-tuples, or a (127, 120; 7) code over binary 6-tuples. Compare this with the distance-7 RS code, which has dimension 121. Only one dimension has been lost in obtaining a cyclic group code over 6-tuples.

D. Decoding

Receive the codeword in 6-tuples and decode for three errors. The decoding algebra is performed in GF(2^7) and the 6-tuples are read as trace-zero elements in their 7-tuple form.

E. Systematic Encoding

An example is presented here, followed by a theorem for general construction.

1. Construction of a Systematic Cyclic Group (15, 10; 5) Code Over Binary Triples. Let $g(x)$ be the generator polynomial of the (15, 11; 5) RS code over GF(16) with α a root of $x^4 + x + 1 = 0$.

$$g(x) = \prod_{i=1}^{3} (x + \alpha^i) = x^4 + \alpha^{12}x^3 + \alpha^4 x^2 + \alpha x + \alpha^6$$

Here the binary 4-tuple (a, b, c, d) represents the field element $\mathbf{u} = a + b\alpha + c\alpha^2 + d\alpha^3$. Binary triples (a, b, c) are treated as elements $a + b\alpha + c\alpha^2$ of GF(16). Note that in GF(16), Tr α = Tr 1 = 0, so the triples belong to the subgroup with elements of trace zero.

Place the 10 information symbols in the first 11 entries, omitting the eighth position for the RS encoder. Now introduce a unique triple called γ in the eighth position and run all 11 triples through the RS encoder to generate four parity symbols, which are elements of trace zero in GF(16). What is this unique γ?

The information triples correspond to the elements α^j, for j = 0, 1, 2, 4, 5, 8, 10, and ∞, where α^∞ denotes the zero additive identity of the field. Note the following set **E** of seven codewords (in powers of α) of the RS code:

∞	∞	∞	∞	∞	∞	∞	0	∞	∞	∞	6	8	7	4
∞	∞	∞	∞	∞	∞	∞	1	∞	∞	∞	7	9	8	5
∞	∞	∞	∞	∞	∞	∞	2	∞	∞	∞	8	10	9	6
∞	∞	∞	∞	∞	∞	∞	4	∞	∞	∞	10	12	11	8
∞	∞	∞	∞	∞	∞	∞	5	∞	∞	∞	11	13	12	9
∞	∞	∞	∞	∞	∞	∞	8	∞	∞	∞	14	1	0	12
∞	∞	∞	∞	∞	∞	∞	10	∞	∞	∞	1	3	2	14

This shows that the information set at the positions 0, 1, 2, 3, 4, 5, 6, 8, 9, and 10 for the triple code consisting of the elements $\{0, 1, 2, 4, 5, 8, 10, \infty\}$ is complete, since only ∞ at position 7 gives a codeword of the (15, 10; 5) code over triples.

2. Explanation. Note for an entry in the eighth position, labeled here (α^7) or "seventh" position (counting from 0 now), the trace-one elements occur in pairs in the parity positions. This is because the RS code has $(x + 1)$ as a factor in its generator polynomial $g(x)$, and so the sums of all symbols add to zero. Note too that all the possible seven ways an even number of trace-one elements can occur do occur. One may take any information set of 10 trace-zero symbols plus ∞ in the "seventh" symbol as a set of information symbols for the RS code generated by $g(x)$. One gets four parity symbols, which must contain an even number of trace-one elements.

Now add a unique codeword γ from the set **E** above to what was just generated. The codeword γ is chosen to eliminate the trace-one elements if they exist in the parity section to obtain a codeword with entries only having trace zero. Note that it is not necessary to store all seven words. In the set **E**, the triples 0, 1, and 8 in the "seventh" position give rise to words with trace one in position pairs (1, 3), (1, 2), and (1, 4). One gets all pair combinations by taking sums of these. Therefore, it is a basis. One need only store three words of size $(3 + 4 + 4 + 4 + 4) = 15$ bits and set up an algorithm for usage. This is a full systematic encoding since the information symbols are transparent and accessible. The general construction will be presented later along with the general case for $(m - j)$-tuple codes of length $2^m - 1$, $j \geq 2$.

The cyclic group codes defined above can be encoded systematically. The encoding will be in two stages: one employing a linear feedback shift register (LFSR) encoder of the RS type and a ROM and perhaps even a second LFSR encoder. Start with an RS code of length $n = 2^m - 1$ over GF(2^m) with distance d. The M-S polynomials for the code are either $P(x) = \sum_{i=0}^{M-1} c_i x^i$ or $Q(x) = \sum_{i=1}^{M} c_i x^i$. A cyclic group code of dimension k over $(m-1)$-tuples and distance $d = n - M + 1$ was defined by using the condition that Tr $P(x) = 0$ or Tr $Q(x) = 0$. Then M' free m-bit constants were obtained where $M'm = k(m - 1)$ for $Q(x)$ and $(M' - 1)k = (m - 1)(k - 1)$ for $P(x)$. In order to systematically encode either case, a theorem is needed for finding a particular set of independent coordinates.

Theorem. Let **A** be a $(2^m - 1,\ k;\ d)$ group cyclic code over binary $(m-1)$-tuples as defined above by a conditioned set on M' coefficients of M-S polynomials $Q(x) = \sum_{i=1}^{M} c_i x^i$, where $M'm = (m-1)k$. If there exists a set of k coordinates with the property that the only codeword in **A** that is zero at these positions is the all-zero codeword, then these coordinates can serve as information symbol positions; i.e., all codewords may be generated from the coordinate values there. Furthermore, if these m points are contained in the first M consecutive positions, one may fill in the $M-m$ missing positions with elements using a ROM and an algorithm and then encode all the n positions from the first M via the usual RS shift-register encoder. The proof is similar for the $P(x)$ type.

Proof: If one has such a set of k coordinates, each of the k^{m-1} possible values taken at these coordinates generates a distinct codeword of **A**. Otherwise, there are at least two codewords of **A** that correspond to some k-tuple. (Note that **A** has k^{m-1} codewords.) If two such codewords are added together, one obtains a nonzero codeword in **A** with zeros at these m positions, which contradicts the hypothesis of the theorem. If the k positions are in consecutive M positions of the codewords, there may be ways to fill something in and use the available RS encoder technology. ❐

A Caveat. If one starts from the polynomial construction of these codes, one has no guarantee that such a set of k coordinates exists. Consider a cyclic code generated by the M-S polynomials $P(x)$; $x = \beta^i$ for $0 \le i \le 14$. Then $P(x) = c_3x^3 + c_3^2x^6 + c_5x^5$; $c_3 \in \mathrm{GF}(16)$, $c_5 \in \mathrm{GF}(4)$. This gives a code of dimension 2 over trace-zero elements (which are represented by triples). It is seen here that two coordinates do not define any triple codeword in a systematic manner.

3. Construction of the (15, 2; 12) Code. List the field elements in powers of β where β is a root of $x^4 + x + 1 = 0$ (∞ denotes the zero of the field). The triples are represented by $(1, 2, 4, 8, \infty, 0, 5, 10)$. Listed here are 35 of the 64 codewords corresponding to $P(\beta^i)$ for $0 \le i \le 14$

∞	2	4	1	8	∞	2	4	1	8	∞	2	4	1	8	(5 shifts)
∞	8	∞	8	0	10	2	5	1	∞	0	4	10	2	10	(15 shifts)
∞	∞	0	1	8	0	5	5	4	4	5	10	∞	2	1	(15 shifts)

Note that ∞ occurs in all pairs of positions and does not satisfy the hypothesis of the theorem. This code cannot be generated systematically from any two positions.

II. Cyclic Group Codes of Length (2^m-1) Over Binary $(m-j)$-tuples, $j \ge 2$

Consider codes of length $2^m - 1$ over j-tuples, where $j \le m-2$ and $\gcd(2^j - 1, 2^m - 1) = 1$. The extension requires no new ideas or theorems but actual definitions and calculations. Appendix B lists a set of these new codes for $k = 5$ and 6. Appendices C and D are constructions of two different codes over binary triples.

To obtain new codes of length $2^m - 1$ over j-tuples, $j < m - 1$:

(1) Represent the j-tuples as subgroups of the trace-zero elements of the field, with m odd and m even treated differently.

(2) Characterize algebraically to preserve cyclicity.

(3) Systematically generate the codes by invoking the theorem.

(4) Note that if $j \mid m$, or $2^j - 1 \mid 2^m - 1$, these are no better than BCH codes. See the example in Appendix C.

Case 1 (m Odd). Find β primitive in the field $\mathrm{GF}(2^m)$ such that $\mathrm{Tr}\ \beta^i = 0$, for $1 \le i \le m-1$. To obtain a subgroup of $(m-2)$-tuples, stipulate that for $\mathbf{a} \in \mathrm{GF}(2^m)$, $\mathrm{Tr}\ \mathbf{a} = \mathrm{Tr}\ \mathbf{a}\beta^{-1} = 0$. To generate subgroups of order $(m-j)$, continue adding $\mathrm{Tr}\ \mathbf{a}\beta^{-i+1} = 0$, $i \le j$ to the previous conditions.

Case 2 (m Even). Find β primitive such that $\mathrm{Tr}\ \beta^j = 0$, $0 \le j < p$ with p as close to $m-1$ as possible. To obtain a subgroup of $(m-2)$-tuples, stipulate that for $\mathbf{a} \in \mathrm{GF}(2^m)$, $\mathrm{Tr}\ \mathbf{a} = \mathrm{Tr}\ \mathbf{a}\beta = 0$. To generate subgroups of order $(m-j)$, continue adding $\mathrm{Tr}\ \mathbf{a}\beta^{i-1} = 0$, $i \le j$ to the previous conditions.

A. Cyclicity

The above conditions ensure cyclicity. For m odd and $j = m-2$, $\mathrm{Tr}\ P(x) = \mathrm{Tr}\ P(x)\beta^{-1} = 0$ for the appropri-

ately chosen β. For the polynomial $P(x) = \sum c_i x^i$, $i = 1$, 2, 4, and 8, the above conditions lead to the equations

$$c_1^8 + c_2^4 + c_4^2 + c_8 = 0$$

$$\beta^{-8} c_1^8 + \beta^{-4} c_2^4 + \beta^{-2} c_4^2 + \beta^{-1} c_8 = 0$$

Shift the $P(x)$ codeword r positions to the left. The new set of coefficients for the shifted word is $P'(x) = \sum d_i x^i$, $d_i = c_i \beta^{ri}$. A simple calculation verifies that the d_i's meet the conditions above.

B. Systematic Encoding

The theorem states that a set of k coordinates can serve as a basis for the group code if there are no nonzero codewords over j-tuples that are zero at these coordinates. Let these k coordinates be the information coordinates. Now if these k's happen to fall in any set of k' consecutive coordinates where k' is the degree of the M-S polynomial of the linear cyclic code over the full field, one may encode systematically by using the encoding shift register plus the small size ROM template that fills in the missing $(k' - k)$ values plus the remaining parity symbols. The technique is similar to the $(m - 1)$-tuple case.

1. Example of Construction of a (31, 25; 5) Code Over Binary Triples. Construct the field GF(32) by choosing β as a root of $x^5 + x^3 + 1 = 0$. The trace-zero elements are 1, 2, 4, 8, 16, 3, 6, 12, 24, 17, 15, 30, 29, 27, 23, and ∞ (the zero identity of the field). The trace-one elements are 0, 5, 10, 20, 9, 18, 11, 22, 13, 26, 21, 7, 14, 28, 25, and 19. Take a set of elements $\mathbf{a} \in$ GF(32) with Tr $\mathbf{a}$ = Tr $\mathbf{a}\beta^{-1} = 0$. There are eight elements here and they are (in powers of β) 2, 3, 4, 16, 17, 24, 30, and ∞. Represent GF(32) by 5-tuples (a, b, c, d, e) corresponding to $\mathbf{a} = a + b\beta + c\beta^2 + d\beta^3 + e\beta^4$. The triples to encode are now $(0, 0, c, d, e)$ in this representation. The generator polynomial for the (31, 27; 5) RS code over GF(32) is given by $g(x) = \prod_{j=0}^{3} (x + \beta^j)$. Explicitly, $g(x) = x^4 + \beta^{11}x^3 + \beta^{20}x^2 + \beta^{14}x + \beta^6$.

Consider the RS codewords given by

∞	∞	∞	...	∞	∞	∞	∞	0	∞	∞	22	25	18	23
∞	∞	∞	...	∞	∞	∞	0	∞	∞	∞	13	27	22	28

From the above, it can be shown that if the coordinates 0–22, 25, and 26 (skipping 23 and 24) are chosen as information positions, they are a basis for group-code generation. To see this, multiply both sequences by the eligible triples and verify that one does not obtain a codeword that contains all triples.

2. Encode. Take any information sequence of triples, place ∞ in positions 23 and 24, and generate a codeword of the full RS code. Examine the four parity symbols for nontriple elements and add the proper unique codeword of the form

$$\infty\infty\infty\infty\infty\infty\infty\infty\infty\infty\infty\ldots ab\infty\infty cdef$$

so that a and b are triples chosen such that c, d, e, and f have ones in same first two positions as the first codeword. That such a word exists is guaranteed below. First, count the dimension of the triple code.

3. Dimension Counting. The conjugate class of 1 2 is 1 2 4 8 16. Since three dimensions are needed to get one, only one dimension is extracted from this class. Now consider the class containing three dimensions. There are four elements left, so two can be extracted, giving a total of 3 × 5 bits, which in symbols equals five (triples) in dimension. There is a BCH code of dimension 20 that has $d = 5$, so the total triple dimension is $20 + 5 = 25$. To verify the encoding, first an even number of elements $\mathbf{a}$ with Tr $\mathbf{a} = 1$ must occur in the four parity symbols. The RS encoder has $(x + 1)$ in the generator polynomial. Secondly, an even number of Tr $\mathbf{a}\beta^{-1} = 1$ must occur for the same reason. There are at most 8 × 8 such combinations. Now the elements a and b in these positions give rise to 64 different word possibilities and they must all yield different possible patterns, otherwise one would get a codeword of triples generated by $\infty\infty\infty\infty\infty\infty\infty\infty\infty\infty\infty\ldots ab\infty\infty cdef$, which, as has been seen, is impossible by sheer calculation.

C. Optimality of These Codes

One wonders how efficient or optimal these codes are. One can compare them with RS codes having the same number of parity checks and see how they differ, or look at BCH codes that have the same number of parity checks. Then there is always the simple Hamming bound to fall back on. For a length $n = 2^k - 1$, and field elements of

$q = n + 1$ elements, the t-error correcting code will have dimension r where

$$q^r \leq q^n / \left[1 + nq + \binom{n}{2} q^2 + \cdots + \binom{n}{t} q^t\right]$$

where $\binom{n}{j} = n!/j!(n-j)!$, which approximates roughly to

$$q^r = q^n / \left[\binom{q}{t} q^t\right] = q^{n-t} / \binom{q}{t}$$

or $r \leq n - t - \log_q \binom{q}{t}$. It is known that for the RS codes, $r = n - 2t$. Now for j-tuples, $q = 2^j$ and $n = 2^m - 1$. An examination of the codes (15, 10; 5) over triples, (31, 26; 5) over 4-tuples, and (63, 56; 7) over 5-tuples shows that they are close to the Hamming bound.

Appendix A

Cyclic Codes of Length $2^m - 1$ Over $(m-1)$-tuples

Cyclic Group Codes of Length 15 Over Binary Triples:

$(15, 5; 9), (15, 10; 5), (15, 7; 7)$

Cyclic Group Codes of Length 31 Over Binary 4-tuples:

$(31, 6; 23), (31, 10; 19), (31, 16; 13), (31, 21; 9), (31, 26; 5)$

Cyclic Group Codes of Length 63 Over Binary 5-tuples:

$(63, 7; 51), (63, 12; 45), (63, 19; 37), (63, 24; 31), (63, 28; 27), (63, 33; 25),$
$(63, 36; 21), (63, 42; 17), (63, 47; 13), (63, 51; 9), (63, 56; 7)$

Appendix B

Cyclic Codes of Length $2^m - 1$ over j-tuples, $j \leq m - 2$

$m = 5$, $j = 3$. Codes over binary triples:

(31, 6; 21), (31, 10; 15), (31, 16; 11), (31, 21; 7), (31, 25; 5)

$m = 5$, $j = 2$. Codes over binary doubles:

(31, 6; 15), (31, 11; 13), (31, 16; 9), (31, 20; 7)

$m = 6$, $j = 4$. Codes over binary 4-tuples:

(63, 7; 47), (63, 12; 39), (63, 18; 31), (63, 22; 27), (63, 28; 25), (63, 30; 21), (63, 35; 21), (63, 41; 15), (63, 47; 11), (63, 51; 9), (63, 57; 5)

Appendix C

Construction of the (15, 7; 7) Group Cyclic Code Over Triples

Let β be a root of x^4+x+1, with β a primitive generator of GF(16). List the field elements as powers of β and let ∞ denote the additive 0 of the field. The trace-zero elements as integer powers of β are ∞, 0, 1, 2, 4, 8, 5, and 10.

Construct the M-S polynomials of degree 8, which give rise to the (15, 9; 7) RS code. Set the coefficient of x^7 equal to zero and consider the check polynomial $f(x) = \prod (x + \beta^j)$; j =0, 1, 2, 4, 8, 3, 6, 5, and $f(x) = (x+1)(x^4+x+1)(x+\beta^3)(x+\beta^6)(x+\beta^5)$. This polynomial written in ascending powers of x has coefficients $[14, 0, 7, \infty, 7, 14, 4, 4, 0]$.

The following codewords illustrate that the information symbol coordinates can be chosen as 0, 1, 2, 3, 4, 5, and 7. (See the theorem.)

∞	∞	∞	∞	∞	∞	0	∞	4	6	14	10	1	11	5
∞	∞	∞	∞	∞	∞	1	∞	5	7	0	11	2	12	6
∞	∞	∞	∞	∞	∞	2	∞	6	8	1	12	3	13	7
∞	∞	∞	∞	∞	∞	4	∞	8	10	3	14	5	0	9
∞	∞	∞	∞	∞	∞	5	∞	9	11	4	0	6	1	10
∞	∞	∞	∞	∞	∞	8	∞	12	14	7	3	9	4	13
∞	∞	∞	∞	∞	∞	10	∞	14	1	9	5	11	6	0

One sees that 0, 1, 2, 3, 4, 5, 7 can serve as an information set for the triples, since there does not exist a nonzero word that is zero at these positions. Still, an algorithm would be preferable so that the codewords can be systematically generated via the modified (15, 8; 7) RS code generated by $f(x)$. For this, a means is needed of generating a triple value at position 6 that depends on the values at positions 0, 1, 2, 3, 4, 5, and 7. This can be achieved by using a ROM indexed by position and triple value at that position. This would be a 9-bit ROM (3 bits for position, 3 bits for the triple at that position, and 3 bits for the triple to be placed in position six). To obtain this ROM requires calculation beforehand.

The contents are listed with positions labeled from 0 to 7 (omitting 6), and triples listed by values (a, b, c) corresponding to $a + b\beta + c\beta^2$. In Table C-1 are shown only 21 such listings at the 0, 1, and 2 powers of β since these serve as a basis for the trace-zero elements. Thus, the 9-bit ROM generates for each triple at each information position the values that are added to form an element placed in the sixth position of the encoding shift register.

A second encoding technique arises from this calculation and is guaranteed by the theorem. Place the information triples along with ∞ in the sixth position and generate the remaining seven 4-tuples in GF(16). From the 4-tuples, extract a 7-tuple corresponding to the trace-one coefficient of β^3. Place this 7-bit element in a 7×3 ROM, which generates a triple to cancel the trace-one elements. Have this triple index a second ROM, which generates seven triples (see the table, which verifies the conditions of the theorem) to be added to the seven-triple portion of parity that has been generated.

Table C-1. Listings at the 0, 1, and 2 powers of β.

Position	Value	Parity at 6
0	0	5
0	1	∞
0	2	4
1	0	0
1	1	4
1	2	0
2	0	5
2	1	0
2	2	5
3	0	0
3	1	4
3	2	0
4	0	5
4	1	0
4	2	5
5	0	10
5	1	4
5	2	1
7	0	∞
7	1	0
7	2	8

Appendix D

(15, 12; 3) Cyclic Code Over Binary Doubles

There are several ways to obtain this code. The standard method involves using the BCH code over GF(4). The generator polynomial has roots 1, β, and β^4, where β is a root of $x^4 + x + 1 = 0$. An alternative is to identify the binary doubles with the set of elements in GF(16) (a, b) corresponding to $a + b\beta$. The (15, 12; 3) code is then made up of the BCH (15, 10; 4) over GF(4) with generator polynomial $x^5 + x^4 + x^2 + 1$.

Add one of the 15 codewords generated by $(x + \beta^7)(x + \beta^{11})(x + \beta^{13})$ using the conditions coming from the above exposition. These words turn out to be any cyclic shift of

$$1, \beta, 1, \beta, \beta^4, 1, \infty, \beta, 1, \infty, \infty, \beta, \beta^4, \beta^4, \beta^4$$

Note that these binary doubles correspond to $\infty, 1, \beta$ and β^4. It would be interesting to see if these codes are isomorphic once the two sets of binary doubles are identified. The BCH code has a simpler encoding.